# Deploying QKD in Standard Optical Networks

D. Lancho[1], J. Martinez-Mateo[1], D. Elkouss[1], A. Ciurana[1], M. Soto[2] and V. Martin[1]*

[1] Facultad de Informática, Universidad Politécnica de Madrid
Campus de Montegancedo, 28660, Boadilla del Monte (Madrid), Spain
[2] Depto. Seguridad en Redes y Servicios, Telefónica Investigación y Desarrollo,
Emilio Vargas 6, Madrid 28043, Spain.
*e-mail: vicente@fi.upm.es web: http://gcc.ls.fi.upm.es

In order to deploy QKD in a cost effective and scalable way, its integration with already installed optical networks is a logical step. If, for the sake of security, we require that no intermediate trusted nodes would be needed, the maximum distance/absorptions allowed by QKD systems limit ourselves to metropolitan area networks. Current metro networks are mostly all optical and passive, hence a transparent link can be established among any two points and this link can be used to transport the quantum channel. In this poster we report on our findings studying the problems arising when integrating QKD systems in standard telecommunications networks.

## 1 Network Testbed

The testbed setup is depicted in Fig. 1. The core has a ring topology and the access has a tree topology. The access currently uses the GPON standard, although DWDM-PON studies are under way. QKD equipments are id Quantique Clavis 3000 and 3100 two way systems using BB84. Mean photon number was set to simulate a decoy state protocol with signal plus one decoy. The optimal mean number for our setup was 0.79. A full protocol stack, including specifically designed LDPC error correction codes with 1.05 efficiency[1][2] and privacy amplification was used.

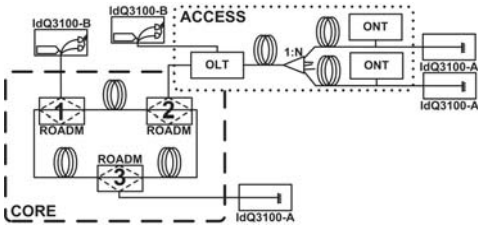


Fig. 1. General testbed network scheme. Enclosed in dashed line is the core part and in dotted line, the access. This testbed is designed to resemble the real PON networks currently used and being deployed by the Telecommunication companies.

In this experiment, a continuous data flux was established among the OLT (core side) and ONT (client side) using the 1490 nm (downstream) and 1310 nm (upstream) channels. Again, QKD used the 1550 nm channel. In this set up, the launch power is fixed and only a small attenuation can be introduced in the OLT. The filtering used was the same (50 GHz) and the splitting factor was four. Losses without fiber are 9 dB. The setup is shown in Fig. 2. It is important to note that in this scheme one Bob can work in time division multiplexing with several Alices, thus reducing the deployment costs of the network.

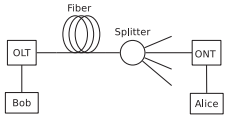


Fig. 2. Access network setup used for the experiment. Bob (in the two-ways paradigm it has the laser and the detectors) is connected to the OLT at the Telecommunication's company premises, where it is multiplexed with the classical channels. A shared fibre connects it with an optical splitter, close to the end user. Finally, an user dedicated fibre goes to the final destination, where is located the OLT and Alice.

The core testbed uses CWDM technology and is composed of three standard ROADM nodes. Two wavelengths, 1510 and 1470 nm are used for classical signals, while 1550 nm is reserved for the quantum channel. Beyond power management, extra filtering to further isolate the quantum channel was needed and standard DWDM 50 GHz (0.4 nm) filters were used. Losses in this scenario, without the fibers are 8 dB. The setup is depicted in Fig. 3

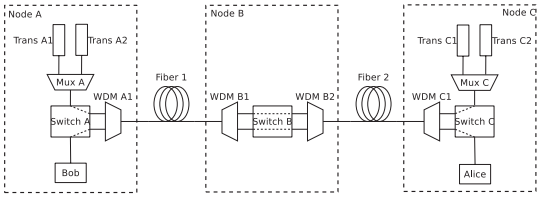


Fig. 3. Core network setup used for the experiment. It is composed by three ROADM nodes. In the first one, Bob is connected to the network. The quantum channel then travels through the shared fibre to the second node, which is configured in pass-through for the quantum channel. After a second shared fibre it reaches the third node, where the quantum channel is dropped to Alice.

## 2 Results

The results of the core network are shown in Fig. 4. Extrapolated data to a 5.6 GHz filtering scheme are included. QBER (left scale) and key rate (right) are presented as a function of the fiber length connecting ROADM nodes 1 and 2, an almost worst case configuration for QKD. The net key throughput is greatly enhanced using the narrower filter, more markedly at the higher distances because the Raman scattering reaching the detectors is still increasing with distance for that fiber length.

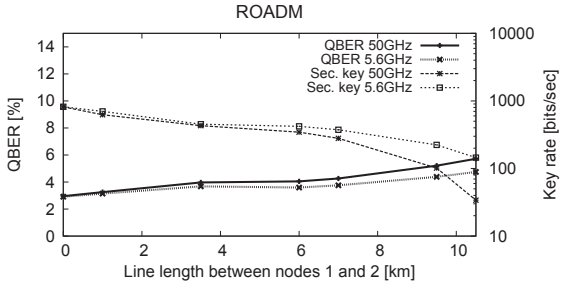


Fig. 4. Core network. For two different filtering are shown the QBER and the final key rate.

In Fig. 5, we present the results for the access network. QBER and key rate is shown as a function of fiber length connecting the OLT with the splitter, again an almost worst case configuration for QKD. In this scenario, the narrower filter is more important because of the unattenuated upstream classical channel. In both scenarios a secure key throughput of over 100 bit/s. is achievable at the longest distances. This is able to sustain an AES256 with a key change rate higher than is usual today and supports the view that the integration of QKD in modern optical networks, although not free from problems, is a real possibility.

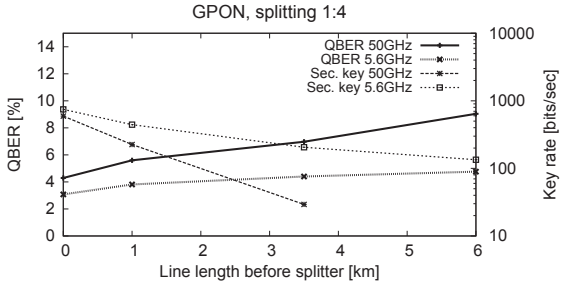


Fig. 5. Access network. For two different filtering are shown the QBER and the final key rate.

## 3 Conclusions

We have shown that QKD in Standard Optical Networks is a real possibility, although it is limited to a short range and therefore to metropolitan area networks. We believe that switched networks, whether sharing the fibers with other classical, quantum or both, channels is the next logical step and a need to deploy QKD in a cost-effective way.
In future experiments we plan to measure the capabilities and limits of different setups of PON networks and new standards being deployed (WDM-PON) with QKD.

## Acknowledgments

This project is partially funded by CDTI, Ministry of Trade and Industry of Spain, under Project Segur@: CENIT-2007 2004 and by project Quantum Information Technologies Madrid (http://www.quitemad.org), P2009/ESP-1594, Comunidad Autónoma de Madrid

## References

[1] D. Elkouss, J. Martinez, D. Lancho, and V. Martin, "Rate compatible protocol for information reconciliation: An application to qkd," *IEEE Information Theory Workshop (ITW)*, pp. 145–149, Jan 2010.

[2] D. Elkouss, J. Martinez-Mateo, D. Lancho, and V. Martin, "Information reconciliation for quantum key distribution," *Somewhere in this poster session!!*